UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/611,809	07/07/2000	David K. Chin	2875.0640001	6867

26111 7590 12/31/2007

STERNE, KESSLER, GOLDSTEIN & FOX P.L.L.C.
1100 NEW YORK AVENUE, N.W.
WASHINGTON, DC 20005

EXAMINER	
COLIN, CARL G	

ART UNIT	PAPER NUMBER
2136	

MAIL DATE	DELIVERY MODE
12/31/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	09/611,809	CHIN ET AL.	
	Examiner	Art Unit	
	Carl Colin	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *21 September 2007*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1,2,4,7-9,12 and 14-30* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1,2,4,7-9,12 and 14-30* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Continued Examination Under 37 CFR 1.114

1. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 9/21/2007 has been entered.

Response to Arguments

2. In response to communications filed on 9/21/2007, applicant amends claims 1-2, 4, 7-9, 12, 14-30. The following claims 1-2, 4, 7-9, 12, 14-30 are presented for examination.

2.1 Applicant's arguments, filed on 9/21/2007, with respect to the rejection of claims 1-2, 4, 7-9, 12, 14-30 have been fully considered, but they are not persuasive. Applicant argues that Hobson does not teach nor suggest at least two multipliers connected to a system memory for multiplying data provided by the system memory and at least one adder connected directly with the at least two multipliers because figure 2 shows a multiplexer MX3 is coupled between a multiplier MUL1 and adder ADD1. Examiner respectfully disagrees with applicant's interpretation of figure 2 and its written description because applicant did not consider the other multipliers such as mul2. For instance, Hobson discloses inputs to multipliers Mul1 and Mul2 using the values stored in the storage areas (see column 6, lines 36-42). See also Fisher, fig. 2B.

Applicant also argues that Fisher does not disclose multiplication may be performed separately from multiply-add operation. Examiner respectfully disagrees as Fisher discloses a decode unit issuing instructions to the execution unit to perform specific arithmetic operations (column 7, lines 23-33). Examiner's interpretation is clearly explained in *US Patent 6,385,634 to Peleg et al, column 7, lines 5-42 and figure 1* as previously mentioned in the last office action. *Peleg et al* provides examples on how the execution units performs specific operations such as multiply-add as well as multiplication, addition, subtraction, etc. according to the instructions received from the decode unit. Applicant has not overcome the rejection of the claims as amended. Upon further consideration, the rejection of claims 1, 2, 4, 7-9, 12, and 14-30 is set forth below.

Claim Rejections - 35 USC § 112

3. The following is a quotation of the first paragraph of 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

Claims 1, 2, 4, 7-9, 12, and 14-30 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the enablement requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to enable one skilled in the art to which it pertains, or with which it is most nearly connected, to make and/or use the invention. The multiplication units are configured to perform multiplication operations in parallel but they are not configured to perform simultaneous multiplication and addition operations (see applicant's figure 2 with description). The addition operations require the result of the multiplication

operation. Therefore, the claims would not meet the enablement requirement to perform multiplication while performing the addition operations. The language of "performing simultaneous or parallel multiplication and addition operation" in applicant's disclosure is described as an instruction to perform a multiplication first and then the product or result is added to another operand (see page 9 and page 16, lines 4-7).

Claim Rejections - 35 USC § 112

4. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Claims 1, 2, 4, 7-9, 12, and 14-30 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. For instance, claims 1, 21, and 22 recite performing specified multiplication and addition operations in parallel and/or performing simultaneous multiplications and addition operations. It is not clear whether the multiplication operations are performed simultaneously separately from the addition operations that are performed simultaneously or the multiplication operations are performed simultaneously with the addition operations.

Claim 4 recites the server of claim 3. Claim 4 is dependent on a cancelled claim. There is insufficient antecedent basis for this limitation in the claim.

Claim Rejections - 35 USC § 103

5. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1, 2, 4, 9, 12, 14-27 are rejected under 35 U.S.C. 103(a) as being unpatentable over US Patent 6,209,016 to **Hobson et al.** in view of US Patent 6,237,016 to **Fisher et al** in view of ***US Patent 6,385,634 to Peleg et al***, in view of US Patent Publication US 2002/0039420 to **Shacham et al**.

As per claim 1, Hobson et al substantially teaches an encryption processor that can be implemented in a server comprising: *a system memory* (see column 6, lines 36-48) *and a processing unit coupled to said system memory including*: an execution unit configured to execute product and square operations, the execution unit including at least one adder and at least two multipliers (see figures 3-4 and column 6, lines 57-62). **Hobson et al.** discloses *an execution unit such as a co-processor coupled to a decode unit* in figure 6 *configured to execute arithmetic operations to perform product and square operations*; **Hobson et al.** discloses *the execution unit including at least one adder and at least two multipliers* (see figures 3-4) **Hobson et al** further discloses at least two multipliers connected to at least one adder for applying addition operations to outputs of said multipliers and storage areas for providing data for

performing multiplication operations (see column 6, lines 36-42 and figures 2-4) that meets the recitation of said *execution unit including at least two multipliers connected directly with said system memory for multiplying data provided from said system memory and at least one adder connected directly with said at least two multipliers for applying an addition operation to outputs of said at least two multipliers;* **Hobson et al.** discloses *said execution unit configurable to perform specified multiplication operations in parallel and configurable to perform specified multiplication and addition operations in parallel* (see column 6, lines 57-62); **Hobson et al.** discloses determining whether a square operation or a product operation is to be performed based on the bit value (see column 6, line 44 through column 7, line 23) that meets the recitation of *determining by the decode unit whether a square operation or a product operation needs to be performed on an operand.* **Hobson et al.** discloses the execution unit performing Montgomery square, which includes performing multiplication operations and discloses performing Montgomery product or multiply which includes performing multiplication and addition operations (see column 6, lines 44-49 and lines 58-67). **Hobson et al.** further discloses performing multiplication and addition operations in parallel to improve performance time (see column 4, lines 27-40 and claim 7) that meets the recitation of *issuing execution to the execution unit so that the execution unit performs specified multiplication and addition operations in parallel and performs specified multiplication operations in parallel while performing either the square or product operation.*

Hobson et al. further suggests using instruction to control operations Hobson discloses a new co-processor that allows to act as a hardware engine capable of performing hardware instructions rather than under software control by the CPU thereby reducing CPU overhead;

"sequence of calculations may be done using a dedicated hardware state machine and arithmetic operations are available within the new co-processor namely addition and subtraction", (see column 7, line 60 through column 8, line 42). Although **Hobson et al** does not explicitly state that the decoder issues the arithmetic instructions to the co-processor, it is understood that the decoder makes the decision as to whether to perform a modular square or a modular multiply and by obviating the need for a CPU, arithmetic instructions are issued directly to the co-processor to the perform specific arithmetic instructions as the new co-processor now includes the arithmetic functions as cited and explained above (see column 6, line 44 through column 8, line 42). **Fisher et al** in an analogous art discloses execution unit including at least two multipliers connected directly with said system memory for multiplying data provided from said system memory and at least one adder connected directly with said at least two multipliers for applying an addition operation to outputs of said at least two multipliers (see fig. 2B) and teaches a decode unit and execution unit for performing instructions and a decode unit issuing instructions to the execution unit to perform specific arithmetic operations (column 7, lines 23-33). Examiner's interpretation is clearly explained in ***US Patent 6,385,634 to Peleg et al, column 7, lines 5-42 and figure 1.*** ***Peleg et al*** provides examples on how the execution units performs specific operations such as multiply-add as well as multiplication, addition, subtraction, etc. according to the instructions received from the decode unit. It would have been obvious to one of ordinary skill in the art at the time the invention was made to use the steps described in **Peleg et al** so as to perform conditional statement operations in the execution units as specified by the decoder unit as suggested by **Fisher et al** (column 7, lines 23-41). **Fisher et al** further discloses first instruction to perform simultaneous multiplication operations and second instruction to perform

simultaneous multiplication-addition operations (see column 8, lines 12-41) one multiplication-addition operation can also be performed at one time in another embodiment (column 9, lines 6-8). **Fisher et al** adds that one of the advantages of this technique is to improve performance in performing complex calculations, for example Fisher discloses in column 7, lines 55-60 completing one or more of packed data instruction including multiple-add instruction in one clock cycle and further discloses complex multiplication to be performed in a single instruction such as multiply-subtract instruction (see column 10, lines 28-30). It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the method of **Hobson** of determining whether to perform a Montgomery square operation or a Montgomery product operation in parallel and performing either the Montgomery square or Montgomery multiplication with the method of **Fisher et al** of issuing specific instruction to perform simultaneous multiplication operations and specific instruction to perform simultaneous multiplication and addition operations to provide a decoder unit issuing instructions comprising a first instruction to perform simultaneous multiplication operations and second instruction to perform simultaneous multiplication and addition operations in performing a square and an additional third instruction to perform simultaneous multiplication and addition operations in performing a multiplication as taught by **Fisher et al**. One of ordinary skill in the art would have been motivated by the suggestions provided by **Fisher et al** to make such a modification because performance of complex operations would improve by performing calculations with fewer decoding instructions (column 9, lines 38-65 and column 10, lines 43-53).

Hobson et al does not explicitly disclose that the co-processor is implemented in a server for client/server message authentication. Official notice is taken by examiner that it would have

been obvious to have the encryption processor configured into a secure web server. This modification would have been obvious because one skilled in the art would have been motivated to implement the encryption processor into a secure web server to establish network security and take advantage of the processor speed in performing Montgomery calculation. **Shacham et al** in an analogous art teaches *a server with a system memory and a processing unit coupled to said system memory* via a system bus, (paragraph 70) the processing unit *obtains values for a modulus N, a private key d, and a cipher text C sent by a client and calculates a value for clear text M for each request for a secure network session made to the server by the client*, (see paragraphs 26-27). It would have been obvious to one of ordinary skill in the art at the time the invention was made to implement the encryption processor of **Hobson et al** into a secure web server configured to perform SSL handshake protocol by deriving a key to convert ciphertext message from client into a clear text message as taught by **Shacham et al**. One of ordinary skill in the art would have been motivated to do so because as known in the art SSL authentication provides a secure communication between client and server on the World Wide Web to guarantee privacy and authenticity of information exchange (see paragraphs 3 and 8).

As per claim 2, the references as combined above disclose the claimed server of claim 1, **Fisher et al** discloses a decode unit and execution unit for performing instructions and a decode unit issuing instructions to the execution unit to perform specific arithmetic operations (column 7, lines 23-33); **Fisher et al** adds that one of the advantages of this technique is to improve performance in performing complex calculations, for example Fisher discloses in column 7, lines 55-60 completing one or more of packed data instruction including multiple-add instruction in

one clock cycle and further discloses complex multiplication to be performed in a single instruction such as multiply-substract instruction (see column 10, lines 28-30) that meets the recitation of wherein said decode unit is configured to issue a set of instructions that causes said execution unit to perform said specified multiplication and operations in parallel to reduce a number of cycles required to perform said product operation. Claim 2 is rejected on the same rationale as the rejection of claim 1.

As per claim 4, Hobson et al. discloses the limitation of wherein certain of said multiplication operations are performed in parallel using a multiply and shift (see column 2, lines 19-49). It is apparent to one skill in the art that certain of the multiplication operations can be processed in parallel as mentioned above by one instruction.

As per claim 9, Official notice is taken by examiner that it would have been obvious to have said encryption processor configured into a secure web server or a secure switch or internet load balance device deploying SSL/TLS or router or VPN gateways or remote access devices used for VPN applications. Therefore, claim 9 is rejected on the same rationale as the rejection of claim 1 above.

As per claim 12, Hobson et al. discloses the limitation of wherein said product and square operations executed by said execution unit are Montgomery product and square operations (see column 1, lines 5-8 and column 2, lines 14-18).

As per claims 14-20, Hobson et al. substantially discloses a co-processor. It is known in the art hardware/software technologies that support encryption processor. Official notice is taken by examiner that it would have been obvious to have the encryption processor configured into a secure web server or a secure switch or internet load balance device deploying SSL/TLS or router or VPN gateways or remote access devices used for VPN applications. **Hobson et al.** does not disclose a secure switch deploying Secure Socket Layer (SSL)/Transport Layer Security (TLS). This modification would have been obvious because one skilled in the art would have been motivated to implement the encryption processor into the examples above to establish network security and take advantage of the processor speed in performing Montgomery calculation.

As per claim 21, Hobson et al substantially discloses a method of performing Montgomery operations that can be used in cryptographic applications wherein said Montgomery comprises: control means for receiving binary data streams and performing modular operation, (see column 11, lines 15-17) that meets the recitation of *receiving by a decode unit a request to perform a modular operation*; It is implicit that instructions are received for the hardware to perform the modular operation, the instructions or signal are interpreted as request. **Hobson et al** discloses the current bit is used to determine whether to perform a modular square or a modular multiply (see column 6, lines 44-49 and lines 58-67) that meets the recitation of *determining by said decode unit whether a square operation or a product operation is to be performed* (see column 6, line 44 through column 7, line 23 for more details). **Hobson et al** discloses *instruction to perform Montgomery square operation and instruction to perform a*

Montgomery product operation (see column 6, lines 44-49 and 58-67 and column 11, lines 15-17). **Hobson et al.** discloses the execution unit performing Montgomery square, which includes performing multiplication operations and discloses performing Montgomery product or multiply which includes performing multiplication and addition operations (see column 6, lines 44-49 and lines 58-67) and further discloses performing multiplication and addition operations in parallel to improve performance time (see column 4, lines 27-40 and claim 7) that meets the recitation of *performing simultaneous multiplication operations and performing simultaneous multiplication and addition operations in response to instruction.* **Hobson et al** discloses a new co-processor that allows to act as a hardware engine capable of performing hardware instructions rather than under software control by the CPU thereby reducing CPU overhead; "sequence of calculations may be done using a dedicated hardware state machine and arithmetic operations are available within the new co-processor namely addition and subtraction", (see column 7, line 60 through column 8, line 42). Although **Hobson et al** does not explicitly state that the decoder issues the arithmetic instructions to the co-processor, it is understood that the decoder makes the decision as to whether to perform a modular square or a modular multiply and by obviating the need for a CPU, arithmetic instructions are issued directly to the co-processor to perform specific arithmetic instructions as the new co-processor now includes the arithmetic functions as cited and explained above (see column 6, line 44 through column 8, line 42).

Fisher et al in an analogous art teaches a decode unit and execution unit for performing instructions and a decode unit issuing instructions to the execution unit to perform specific arithmetic operations (column 7, lines 23-33). Examiner's interpretation is clearly explained in ***US Patent 6,385,634 to Peleg et al, column 7, lines 5-42 and figure 1*** as previously mentioned

in the last office action. ***Peleg et al*** provides examples on how the execution units performs specific operations such as multiply-add as well as multiplication, addition, subtraction, etc. according to the instructions received from the decode unit. It would have been obvious to one of ordinary skill in the art at the time the invention was made to use the steps described in **Peleg et al** so as to perform conditional statement operations in the execution units as specified by the decoder unit as suggested by **Fisher et al** (column 7, lines 23-41). **Fisher et al** further discloses first instruction to perform simultaneous multiplication operations and second instruction to perform simultaneous multiplication-addition operations (see column 8, lines 12-41) one multiplication-addition operation can also be performed at one time in another embodiment (column 9, lines 6-8). **Fisher et al** adds that one of the advantages of this technique is to improve performance in performing complex calculations, for example Fisher discloses in column 7, lines 55-60 completing one or more of packed data instruction including multiple-add instruction in one clock cycle and further discloses complex multiplication to be performed in a single instruction such as multiply-subtract instruction (see column 10, lines 28-30). It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the method of **Hobson** of determining whether to perform a Montgomery square operation or a Montgomery product operation in parallel and performing either the Montgomery square or Montgomery multiplication with the method of **Fisher et al** of issuing specific instruction to perform simultaneous multiplication operations and specific instruction to perform simultaneous multiplication and addition operations to provide a decoder unit issuing instructions comprising a first instruction to perform simultaneous multiplication operations and second instruction to perform simultaneous multiplication and addition operations in performing

a square and an additional third instruction to perform simultaneous multiplication and addition operations in performing a multiplication as taught by **Fisher et al**. One of ordinary skill in the art would have been motivated by the suggestions provided by **Fisher et al** to make such a modification because performance of complex operations would improve by performing calculations with fewer decoding instructions (column 9, lines 38-65 and column 10, lines 43-53).

Hobson et al does not explicitly disclose that the co-processor is implemented in a server for client/server message authentication. Official notice is taken by examiner that it would have been obvious to have the encryption processor configured into a secure web server. This modification would have been obvious because one skilled in the art would have been motivated to implement the encryption processor into a secure web server to establish network security and take advantage of the processor speed in performing Montgomery calculation. **Shacham et al** in an analogous art teaches *a method to establish a secure network session comprising sending an encrypted message to a server using a public key and decrypting said encrypted message by the server using a private key* (see paragraph 27); *generating key to encrypt/decrypt wherein generation of the key further comprises modular exponentiation operation* (the processing unit obtains values for a modulus N, a private key d, and a cipher text C sent by a client and calculates a value for clear text M for each request for a secure network session made to the server by the client) (see paragraphs 26-27). It would have been obvious to one of ordinary skill in the art at the time the invention was made to implement the encryption processor of **Hobson et al** for performing Montgomery modular operation into a secure web server configured to perform SSL handshake protocol by deriving a key to convert ciphertext message from client

into a clear text message as taught by **Shacham et al**. One of ordinary skill in the art would have been motivated to do so because as known in the art SSL authentication provides a secure communication between client and server on the World Wide Web to guarantee privacy and authenticity of information exchange (see paragraphs 3 and 8).

As per claim 22, Hobson et al substantially discloses a method of performing Montgomery operations that can be used in cryptographic applications wherein said Montgomery comprises: *determining whether to perform a modular square or a modular multiply* (see column 6, lines 44-49 and lines 58-67 and column 11, lines 15-17) that meets the recitation of determining by the decode unit whether a square operation or a product operation is to be performed (see column 6, line 44 through column 7, line 23 for more details). **Hobson et al** discloses *instruction to perform Montgomery square operation and instruction to perform a Montgomery product operation* (see column 6, lines 44-49 and 58-67 and column 11, lines 15-17). **Hobson et al.** discloses the execution unit performing Montgomery square, which includes performing multiplication operations and discloses performing Montgomery product or multiply which includes performing multiplication and addition operations (see column 6, lines 44-49 and lines 58-67) and further discloses performing multiplication and addition operations in parallel to improve performance time (see column 4, lines 27-40 and claim 7) that meets the recitation of *performing simultaneous multiplication operations and performing simultaneous multiplication and addition operations in response to instruction.* **Hobson et al** discloses a new co-processor that allows to act as a hardware engine capable of performing hardware instructions rather than under software control by the CPU thereby reducing CPU overhead; "sequence of calculations

may be done using a dedicated hardware state machine and arithmetic operations are available within the new co-processor namely addition and subtraction", (see column 7, line 60 through column 8, line 42). Although **Hobson et al** does not explicitly state that the decoder issues the arithmetic instructions to the co-processor, it is understood that the decoder makes the decision as to whether to perform a modular square or a modular multiply and by obviating the need for a CPU, arithmetic instructions are issued directly to the co-processor to perform specific arithmetic instructions as the new co-processor now includes the arithmetic functions as cited and explained above (see column 6, line 44 through column 8, line 42).

Fisher et al in an analogous art teaches a decode unit and execution unit for performing instructions and a decode unit issuing instructions to the execution unit to perform specific arithmetic operations (column 7, lines 23-33). Examiner's interpretation is clearly explained in ***US Patent 6,385,634 to Peleg et al, column 7, lines 5-42 and figure 1*** as previously mentioned in the last office action. ***Peleg et al*** provides examples on how the execution units performs specific operations such as multiply-add as well as multiplication, addition, subtraction, etc. according to the instructions received from the decode unit. It would have been obvious to one of ordinary skill in the art at the time the invention was made to use the steps described in **Peleg et al** so as to perform conditional statement operations in the execution units as specified by the decoder unit as suggested by **Fisher et al** (column 7, lines 23-41). **Fisher et al** further discloses first instruction to perform simultaneous multiplication operations and second instruction to perform simultaneous multiplication-addition operations (see column 8, lines 12-41) one multiplication-addition operation can also be performed at one time in another embodiment (column 9, lines 6-8). **Fisher et al** adds that one of the advantages of this technique is to

improve performance in performing complex calculations, for example Fisher discloses in column 7, lines 55-60 completing one or more of packed data instruction including multiple-add instruction in one clock cycle and further discloses complex multiplication to be performed in a single instruction such as multiply-subtract instruction (see column 10, lines 28-30). It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the method of **Hobson** of determining whether to perform a Montgomery square operation or a Montgomery product operation in parallel and performing either the Montgomery square or Montgomery multiplication with the method of **Fisher et al** of issuing specific instruction to perform simultaneous multiplication operations and specific instruction to perform simultaneous multiplication and addition operations to provide a decoder unit issuing instructions comprising a first instruction to perform simultaneous multiplication operations and second instruction to perform simultaneous multiplication and addition operations in performing a square and an additional third instruction to perform simultaneous multiplication and addition operations in performing a multiplication as taught by **Fisher et al**. One of ordinary skill in the art would have been motivated by the suggestions provided by **Fisher et al** to make such a modification because performance of complex operations would improve by performing calculations with fewer decoding instructions (column 9, lines 38-65 and column 10, lines 43-53).

Hobson et al does not explicitly disclose that the co-processor is implemented in a server for client/server message authentication. Official notice is taken by examiner that it would have been obvious to have the encryption processor configured into a secure web server. This modification would have been obvious because one skilled in the art would have been motivated

to implement the encryption processor into a secure web server to establish network security and take advantage of the processor speed in performing Montgomery calculation. **Shacham et al** in an analogous art teaches *a method to establish a secure network session comprising sending an encrypted message to a server using a public key and decrypting said encrypted message by the server using a private key* (see paragraph 27); *generating key to encrypt/decrypt wherein generation of the key further comprises modular exponentiation operation* (the processing unit obtains values for a modulus N, a private key d, and a cipher text C sent by a client and calculates a value for clear text M for each request for a secure network session made to the server by the client) (see paragraphs 26-27). It would have been obvious to one of ordinary skill in the art at the time the invention was made to implement the encryption processor of **Hobson et al** for performing Montgomery modular operation into a secure web server configured to perform SSL handshake protocol by deriving a key to convert ciphertext message from client into a clear text message as taught by **Shacham et al**. One of ordinary skill in the art would have been motivated to do so because as known in the art SSL authentication provides a secure communication between client and server on the World Wide Web to guarantee privacy and authenticity of information exchange (see paragraphs 3 and 8).

As per claims 23-25, the references as combined above disclose an apparatus comprising of at least one adder and at least two multipliers (**Fisher et al**, column 9, lines 1-7) performing two specified multiplications in parallel using only one multiply-add instruction (**Fisher et al**, column 9, line 15 through column 10, line 53) that meets the recitation of said least one adder and at least two multipliers perform said specified multiplication operations in parallel in a first

clock cycle. **Fisher et al** also suggests as alternative embodiment an apparatus capable of performing in one instruction multiply-add operation in combination with some other operation (column 10, lines 43-53). **Fisher** also discloses in column 7, lines 55-60 completing one or more of packed data instruction including multiple-add instruction in one clock cycle and further discloses complex multiplication to be performed in a single instruction such as multiply-substract instruction (see column 10, lines 28-30). Regarding the limitation of claim 25, as it is known in the art for the processor to perform operations, instructions are given to the processor as to what operations need to be performed, therefore as indicated in both references specified instructions are given to perform specified functions (see **Fisher et al,** code examples in columns 23-26, claim 9 and column 7, lines 23-41 and column 16, lines 18-67). Examiner's interpretation is clearly explained in ***US Patent 6,385,634 to Peleg et al, column 7, lines 5-42 and column 13, lines 3-22, 45-48. Peleg et al*** provides examples on how the execution units performs specific operations such as multiply-add as well as multiplication, addition, substraction, etc. according to the instructions received from the decode unit. It would have been obvious to one of ordinary skill in the art at the time the invention was made to use the steps decribed in **Peleg et al** so as to perform conditional statement operations in the execution units as specified by the decoder unit as suggested by **Fisher et al** (column 7, lines 23-41). Also **Fisher et al** discloses a multiply-accumulate operation can perform multiplication operation and the result is added for an addition operation (column 15, lines 38-43). Alternative embodiment with different instruction name or different instructions and different combination of operations are within the scope of the teaching of Fisher (column 9, lines 60-67 and column 16, lines 56-58) as known in the art a multiplication and an addition operation can be performed in a single instruction similar to a calculator

program. Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the disclosure of **Hobson** of using apparatus or software control for controlling the sequence of operations as indicated in column 8, lines 1-41 and determining whether to perform a Montgomery square operation or a Montgomery product operation in parallel and performing either the Montgomery square or Montgomery multiplication with the method of **Fisher et al** of issuing specific instruction to perform simultaneous multiplication operations and specific instruction to perform simultaneous multiplication and addition operations to provide a decoder unit issuing instructions comprising a first instruction to perform simultaneous multiplication operations and second instruction to perform simultaneous multiplication and addition operations in performing a square and an additional third instruction to perform simultaneous multiplication and addition operations in performing a multiplication as taught by **Fisher et al**. One skilled in the art would have been lead to make such a modification because the performance of complex operations such as Montgomery operations would improve by performing several calculations with fewer decoding instructions as suggested by **Fisher et al** (column 9, lines 38-45 and column 10, lines 43-53).

Claims 26-27 discloses similar limitation as found in claim 1, except for using modular operation; however, the references also disclose operation to be performed on operand for a modular operation. Therefore, claims 26-27 are rejected on the same rationale as the rejection of claims 1 and 23-25.

As per claim 28, the references as combined above disclose wherein the arithmetic instructions comprise a set of micro instructions (see **Hobson et al**, column 6, lines 57-67, column 7, lines 20-24; and column 8, lines 1-20) and (**Fisher**, column 7, line 40 through column 8, line 35).

As per claim 29, the references as combined above disclose wherein said arithmetic instructions comprise a plurality of types of add-substract instructions and a plurality of types of multiply instructions (see **Hobson et al**, column 6, lines 57-67, column 7, lines 20-24; and column 8, lines 1-20) and (**Fisher**, column 7, line 40 through column 8, line 35).

As per claim 30, the references as combined above disclose wherein the value for clear text M is calculated using the Montgomery method (see **Hobson et al**, column 1, lines 10-49), **Hobson et al** discloses the importance of using Montgomery method for cryptographic applications and key generation; keys are used for encrypting/decrypting meaning changing ciphertext to clear text, which meets the recitation of claim 30. Therefore, claim 30 is rejected on the same rationale as the rejection of claim 1.

6. **Claims 7-8** are rejected under 35 U.S.C. 103(a) as being unpatentable over US Patent 6,209,016 to **Hobson et al.** in view of US Patent 6,237,016 to **Fisher et al** in view of ***US Patent 6,385,634 to Peleg et al,*** in view of US Patent Publication US 2002/0039420 to **Shacham et al** as applied to claim 1 and further in view of US Patent 6,064,740 to **Curiger et al.**.

6.1 **As per claims 7 and 8, Hobson et al.** discloses the limitation of wherein said decode unit is further configured to decode an operation $M=C^d$ mod N and discloses determining whether to perform a square or multiply; and if the exponent d equals to a first logic state implement a square and a product operation. **Hobson et al.** does not explicitly teach the details of the process. However, **Curiger et al.** in an analogous art teaches (a) determining the MSB position of an exponent d equal to a first logic state and (b) issuing a first set of instructions to implement a square and a product operation after said MSB position of said exponent d equal to the first logic state is determined (see column 11, lines 3-9); (c) determining if a next most significant bit (MSB) of said exponent (d) is of the first logic state or a second logic state; and either (d) issuing a second set of instructions to said execution unit to implement a square operation if said next MSB is of the second logic state; or (e) issuing said first set of instructions to the execution unit if said next MSB of the exponent is of the first logic state instructions to implement a square and a product operation (see column 11, lines 9-15); and repeating (c) through (e) for every bit in the exponent (d) from said next MSB to a least significant bit (LSB) (see column 11, lines 15-25). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the method and apparatus as combined above to apply the instructions as described above and the final result of the operation $M = C^d$ mod N by accumulating the results of (b) through (e) as taught by **Curiger et al.** to maximize the speed of the calculations. This modification would have been obvious because one skilled in the art would have been motivated by the suggestions provided by **Curiger et al.** so as to maximize the speed of the calculations.

Conclusion

7. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure as the prior art discloses circuit with multipliers and adders for performing instructions of multiplication and addition operations in parallel.

7.1 Any inquiry concerning this communication or earlier communications from the examiner should be directed to Carl Colin whose telephone number is 571-272-3862. The examiner can normally be reached on Monday through Thursday, 8:00-6:30 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nasser G. Moazzami can be reached on 571-272-4195. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Carl Colin/
Carl Colin
Patent Examiner, A.U. 2136
December 24, 2007